

FILED

UNITED STATES DISTRICT COURT
DISTRICT OF NEW MEXICO

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

JUN 18 2003

**JAMES SEABA and
CORY PHILLIPS,**

R. Litchfield
CLERK

Plaintiffs,

v.

Civ. No. 02-103 LH/RHS

MESOSYSTEMS TECHNOLOGY, INC.,

Defendant.

**SUPPLEMENTAL AFFIDAVIT OF ANTON M. LITCHFIELD
IN SUPPORT OF DEFENDANT'S REPLY TO PLAINTIFFS' RESPONSE TO
MOTION TO DISMISS**

STATE OF OREGON)
) ss.
COUNTY OF MULTNOMAH)

Anton M. Litchfield, being first duly sworn upon oath, states as follows:

1. I am employed by New Technologies Armor, Inc. ("NTI"), a company specializing in the examination of computer-generated files and media. Since 1996, I have been conducting computer medium examinations with NTI and the Ontario Provincial Police of Toronto, Canada.
2. I have personal knowledge of the matters stated herein.
3. I submit this supplemental affidavit in support of Defendant's Reply to Plaintiffs' Response to Motion to Dismiss Plaintiffs' Complaint and for Attorneys' Fees and Costs as a Sanction for Plaintiffs' Abuse of the Discovery Process.
4. NTI has been retained by MesoSystems Technology, Inc. ("MesoSystems") to maintain custody and control of two computer laptops and to conduct a factual examination of the activity on the hard drives of the laptops after

99

December 6, 2001. From February 12, 2002, when the laptops arrived at NTI, through the present, the laptops have been in the exclusive custody and control of NTI.

5. Neither NTI nor I were involved in setting up and implementing MesoSystems' chain of custody procedures.

6. I have no first-hand knowledge of the whereabouts of the two laptop computers at issue prior to NTI taking possession of them in February 2002. I did not initially handle the computers when they were delivered to NTI. Instead, according to NTI's records, including the Chain of Custody Log from MesoSystems that accompanied the computers, the computers were received and placed into storage by Paul T. French, a Lab Director at NTI.

7. According to NTI's records, the Chain of Custody Log was included in the same box in which the computers were shipped.

8. After receipt of the laptops, NTI did not document its activities with respect to the laptops by making entries on the Chain of Custody Log whenever any NTI employee performed its examination of the hard drives or attempted data recovery. Rather, as described below, all handling of the computers was logged in NTI's database.

9. Generally, when a client sends a computer to NTI for examination, a receptionist signs the receipt of the package delivery. Then, the receptionist notifies the Consulting Department that there is a package waiting. A member of the Consulting Department then takes the package and puts it in a secured storage room. After the package is secured, the consultant receiving the package enters a log of the receipt of the package into NTI's database. For these laptops, Mr. French was the consultant who received and logged in the laptops.

10. In January 2003, NTI first began its examination of the contents of the hard drives contained on the laptops. Sean Barry, a computer forensics specialist, performed the initial analysis of the hard drives. According to NTI's records, Mr. Barry created the original imaging of the hard drives and began the examination of the hard

drives on January 3, 2003 for Seaba's computer and on January 6, 2003 for Phillips' computer.

11. My examination of Seaba's computer also showed that the date and time were ahead by exactly 11 months (correcting for the difference between the time zone in New Mexico and Oregon). For example, if today were June 16, 2003, the date on Seaba's computer would be exactly 11 months ahead of today, so it would be May 16, 2004. There are several possible explanations as to why this may have occurred including, battery going bad, damage to the computer itself, power surge, power spike, and date tampering.

12. My examination of Phillips' computer showed that its date and time were accurate (again correcting for the time zone differences).

13. In order to determine whether date tampering occurred on Seaba's and Phillips' laptops, I relied on a program called "SchedLog." SchedLog is a Windows system file that records the dates and times of events performed by a program called "Task Scheduler." One of these events is when "Task Scheduler" starts. Using Phillips' laptop, I determined that "Task Scheduler" starts (and records in SchedLog) when the computer is booted into Windows Millenium. Task Scheduler is a program that allows the user to set dates and times to run certain programs on his computer.

14. SchedLog works as follows: Every time a computer is turned on (and at certain other times while the computer is running), Windows records the date and time in the SchedLog file in sequence. Windows records the date and time in the SchedLog file by using the system date. If one changes the system date, it results in sequential entries in the SchedLog file that are out of chronological order. For example, if a computer is turned on once per day starting on June 1, 2003, and there is no tampering with the system date, the SchedLog would look like this: June 1, 2003; June 2, 2003; June 3, 2003; June 4, 2003; and so on. However, if on June 4, 2003, the system date was

changed to June 1, 2003, the SchedLog would look like this: June 1, 2003; June 2, 2003; June 3, 2003; June 4, 2003; June 1, 2003; June 2, 2003; and so on.

15. The SchedLog file itself could be altered or obliterated, however any access or modification to SchedLog will change the modification or last access date for that file. The only way to cover that up would be to use specialized software that allows a user to directly access the directory information and then use that software to change the modification/last access dates and times to hide the fact that a change took place. For example, if the last three dates the computer was booted into Windows were: January 2, 2003, January 4, 2003, and January 9, 2003, those would be the last three entries in the Schedlog file. If the date were then tampered with and changed to January 5, 2003 and then booted into Windows, the SchedLog would look like this: January 2, 2003; January 4, 2003; January 9, 2003; and January 5, 2003. If the user even knew SchedLog existed, the user could then simply open SchedLog with a text editor (i.e., Notepad) and delete the entry for January 5, 2003. This however would not hide the fact that the dates had been tampered with as the modification and last access dates would reflect January 5, 2003 instead of January 9, 2003, and would require the user to use specialized software to change the dates and times to match SchedLog.

16. It is highly unlikely that a layperson without extensive knowledge and experience in computer systems would know about the existence and functionality of the SchedLog file. It is even more unlikely that a layperson could manipulate SchedLog in such a way as to hide any tracks that the date and time had been altered. It would take specialized software to change the SchedLog file to alter the date and time without leaving obvious signs that date and time tampering had occurred.

17. I did not find any traces of date or time tampering on either hard drive. In fact, my examination revealed that all of the dates and times in the SchedLog files for both laptops were all temporally sequential. Furthermore, all sequential entries on the SchedLog were in chronological order and there were no anomalies in the temporal

sequence. There was no evidence to suggest that the SchedLog file itself had been accessed or changed. There was no other evidence that the system date or any other dates on the computers had been tampered with.

18. My examination did reveal, however, that both Seaba's and Phillips' notebooks had numerous deleted files, as explained in more detail in my Affidavit in Support of Defendant's Motion to Dismiss. Although NFI discovered that numerous files had been deleted, NFI only recovered files that MesoSystems directed it to recover. Because NFI only recovered files identified by MesoSystems, I did not undertake to recover all deleted files.

19. It is possible that documents could have been printed or the computers could have been simply turned on between December 6, 2001 and January 30, 2002.

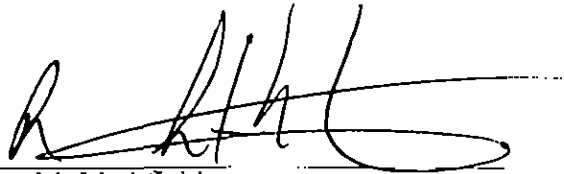
20. The D-drive partition of Seaba's computer had a Windows system folder created on it on September 5, 2001. The D-drive partition of Phillips' computer had a Windows system folder created on it on September 4, 2001. Based on this information, it would appear Seaba's D-drive was created on or before September 5, 2001 and the Phillips' D-drive was created on or before September 4, 2001.

21. Seaba's D-drive contains numerous Office-related files: email messages, a personal letter called IRS.doc that contains an explanation for a mortgage interest discrepancy, and PowerPoint presentations. The PowerPoint presentations located on the D-drive are of particular note. Five PowerPoint presentations, file names _2.01.F3X.ver3.18p Top R Doc.English.ppt, _5.01.F3X Gasoline FP Status Report.ppt, _600.AFI evaluation0613.ppt, _7.01F3X Gasoline FP.final.ppt, _7.01.F3X Gasoline FP.Seaba.final.ppt, show that the author of the presentations as "Honda R&D Americas, Inc." and that the company is "Honda R&D Americas." Each PowerPoint presentation contains a title page or other indication that the presentations were for or by Honda R&D Americas. Two other PowerPoint presentations, file names _7.01.Meso.F3X Gasoline FP.final.ppt and _9.01.Meso.F3X Gasoline.summary.ppt, bear Mesofuel's name

throughout the slides. However, the _7.01.Meso.F3X Gasoline FP.final.ppt file also bears the name of "Honda R&D Americas Fundamental Research Laboratories" on the title page, in addition to "MesoFuel" in the header. This file is exactly the same file as _7.01.F3X Gasoline FP.final.ppt and _7.01.F3X Gasoline FP.Seaba.final.ppt files with the exception that "MesoFuel" is shown in the header. Additionally, the _9.01.Meso.F3X Gasoline.summary.ppt file contains 9 slides that are the same as 9 of the slides in both _7.01.F3X Gasoline FP.final.ppt and _7.01.F3X Gasoline FP.Seaba.final.ppt files, with the exception that "MesoFuel" is shown in the header.

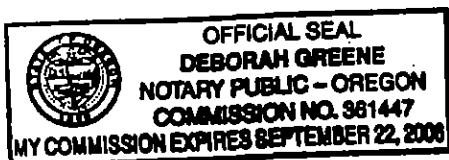
22. Additionally, there are also several files located on Seaba's D-drive, including file names aspen.pdf, bfc.pdf, 108-0843_img.jpg, 108-0842_img.jpg, 10.26 markup of b plan.msg, and blue star nondisclosure agreement.doc. These files were in Seaba's inbox in Microsoft Outlook. Each file was subsequently saved to Seaba's D-drive shortly after (within a few days) receipt in Microsoft Outlook inbox.

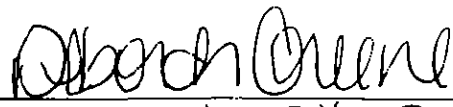
23. Because Seaba's D-drive contains numerous files that are personal to him, it is evident that Seaba must have known how to and did in fact access the D-drive on his laptop.



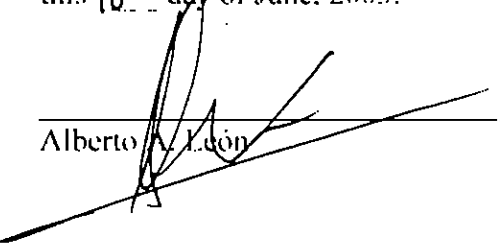
Anton M. Litchfield

SUBSCRIBED and SWORN to before me this 11 day of June, 2003.




 Print Name: Deborah Greene
 Notary Public in and for the State of Oregon,
 residing at Oresham Oregon
 My commission expires: 9/22/2006

I HEREBY CERTIFY that a true
and correct copy of the foregoing
was mailed to counsel of record
this 18th day of June, 2003.



Alberto A. León